range of numbers. Fig. 2 is a high-level depiction of the process, and encompasses this specific embodiment, as well as the more basic case where the credit card numbers are retrieved from a database and then immediately activated.

Having set forth a summary of how the invention can be implemented, further details are provided in the following.

The first thing that the credit card provider should do is to generate a list of additional credit card numbers, whether they be single use or multiple use, and allocate additional credit numbers to a master credit card as a further credit card number for optional use instead of the master credit card number. Such a list can be produced by any suitable software package in the exemplary manner discussed in more detail below. Since the numbers allocated to a particular master credit card holder will not have any link to the master credit card number, the master credit card number should not be able to be derived from the additional credit card numbers.

In effect, randomness in credit card numbers is provided by the fact that there is a queue formed by the customers requiring numbers. Further, it should not be possible, even knowing the additional credit card numbers in a particular master credit card holder's possession which he or she may have used, to predict the next set of numbers that that particular master credit card holder will be allocated, since there will be randomness of access to additional credit card numbers in the truest sense. Even if the credit card provider were to allocate numbers sequentially, there would be no way of predicting the number that that credit card holder would subsequently acquire, since the numbers would be allocated by virtue of a queue, the randomness of this allocation being such as to prevent any prediction.

As such, the credit card numbers generated by the central computer need not be *per se* random numbers. Preferably, though, these numbers are valid credit card numbers with the constraint that they must conform to industry specifications of the format in terms of their numerical content in such a way that they can be handled with no (or minimal) modifications by merchant/acquiring systems and networks and be routed to

the appropriate center for processing. An additional constraint is that they must be different from all other conventional account numbers and all other single use numbers during their lifetime of validity. These constraints are practical requirements to produce a commercially viable system, which would likely not be satisfied by any process that generates random numbers in isolation.

To achieve these allocation requirements, an issuing bank decides within its total available range of credit cards to allocate a certain range or ranges of numbers to the single use system, referred to herein as the "available range." This may represent spare numbers using existing header sequences (e.g., the sequence of usually 4-6 digits that define the issuing institution and are used to route the card to the appropriate transaction processor) or within newly created header sequences. The numbers not allocated include existing credit card accounts for that issuer and sufficient spare capacity for new account holders and replacement numbers for existing customers. The additional non-embossed components of the card details and any card specific information that is transmitted during a transaction may be varied from card to card to enhance security and privacy of credit card transactions.

Although each limited use number is unique during the its lifetime of validity, information required to route the card number and transaction details to the appropriate processor is maintained to ensure that limited use numbers are processed appropriately. However, the limited use numbers do not need to include either the master card account number or an encoded version of the account number. Indeed privacy and security are enhanced when no unique account holder identifier is included within the limited use credit card number.

Also, information that is verified prior to the card being processed for authorization and payment, such as expiry date and checksum digit must be valid. This information may vary from limited use number to limited use number, but must be valid to ensure that the number passes checks that may be completed within the merchant terminal, i.e., the checksum is appropriately calculated for each limited use number and the associated expiry date is valid at the time of use.

Within the constraint of using a valid credit card format, the random allocation process used to generate lists of unique limited use numbers can involve allocation from a range of numbers in which either the entire number or portions of the account number are varied. In addition, the allocation can include combinations of all or part of the account number together with all or part of additional information such as non-embossed additional numbers, expiry date and other information that identifies the card and is passed on by the merchant to the card processor during a transaction.

Sequential random allocation from a list of available valid credit/debit/charge card codes that have been solely allocated for use as limited use numbers ensures that the criteria specified for limited use numbers are met, i.e., no two limited use numbers are the same, no limited use number is the same as an existing account number, and no newly issued conventional card number is the same as a previously issued limited use number. To achieve true computational independence between account numbers and limited use cards and between limited use numbers for the same account, the random allocation process requires a truly random seed value. Such true randomness can be obtained from a physically random system with well defined properties such as a white noise generator. An analog to digital converter that receives an analog signal from such a truly random physical system can be used to ensure truly random allocation.

Other approaches can result in the same result with lower computational efficiency. For example the allocation process could randomly select valid credit card numbers within the entire range for a given card issuer and then discard the number if it is already in use as a limited use or conventional card number or if the same number was allocated within a given time frame.

The above process generates a series of available single use numbers. To repeat, the allocation process is achieved by a truly random (or less ideally a pseudo random) mapping process in which a single use number is randomly selected and then assigned to a selected account holder (either an existing credit/debit card holder, a new solely single use account holder or a bank account). Additional single use

numbers can be allocated for purchase on an individual basis. Each assigned single use number is then removed from the sequence of available numbers before the next allocation, ensuring a unique allocation of each single use number. An alternative mechanism for performing direct allocation to a specific account holder is for lists of single use numbers to be allocated to unique storage locations. The list from a specific storage location can then be directly allocated to a given account at a later date. This allows for rapid allocation of cards to new customers without any delay arising from the need to perform a new allocation procedure for each new customer.

This allocation process generates another series of single use numbers, the "allocated range" with an associated identification field to determine how the account will be settled once used, i.e., onto whose account the transaction will be charged. The allocation process can occur a significant time before the single use numbers are required. Once allocated, they are not added into the list of valid accounts until required by the user.

Fig. 3 is a flow chart illustrating an exemplary process for allocating credit card numbers. A central processing unit (CPU) generates a database of credit card numbers (step 302), and may select a master credit card number. (Step 304). In step 306, the CPU checks to make sure that the master credit card number is not the same as another credit card number. The CPU selects additional credit card numbers to allocate to the master credit card number or other type of account number. (Step 308). The CPU can use any of the techniques discussed above to select the additional numbers. In step 310, the CPU checks to make sure that the additional numbers are not the same as another credit card number. The additional numbers can be used, for example, for single use cards.

When a customer needs single use cards, the CPU can issue the additional credit card numbers to the customer. Unless these single use numbers are issued directly into the hands of the customer (e.g., by an automated teller machine (ATM)), they are not directly added to the list of valid account numbers held within the central computer system. These numbers are added to an "issued, but not valid" list of numbers. (Step

312). The number of single use numbers issued at one time depends upon the rate at which the customer will use the cards and the capability of the device used to store the single use numbers until used. The CPU can provide the customer with enough single use numbers to fulfill their single use purchase requirements for up to, for example, 2 years. Each single use number can be endowed with specific restrictions in terms of transaction type or value, provided that these properties do not exceed the restrictions placed up on the customer's account (such as the available credit balance).

Once a series of single use numbers are issued, the user has the option of confirming receipt by telephone before any of the issued numbers become validated on the processing system. (Step 314). Once receipt has been confirmed (or assumed), not every issued single use number is added to the "issued and valid" list. (Step 316). To prevent excessive valid single use numbers being held within the processing system, the number of single use numbers declared to be valid at any one time is limited to account for waste of numbers (i.e., numbers that are accessed by a customer but are never used to complete a transaction) and to allow for time delays between different transactions leading to differences in the sequence in which single use numbers are accessed by the customer and the sequence in which they arrive at the processing center. The maximum number of single use numbers valid at any one time can be determined by the card issuer but would be preferably in the range of 5-10. In the case of any attempted use outside the allocated range, the next single use number can be used as an additional identifier to validate the transaction. In this case, only a subset of the digits should be given by the user to prevent a fraudulent trader being able to gain access to multiple unused single use numbers. As soon as a single use number is invalidated (step 320) on use (step 318), an additional number from the "issued not valid" list for that customer is allocated to the "issued and valid" list, ensuring a continual supply of single use numbers up to the maximum allowed until the next set of single use numbers are issued. (Step 322).

In relation to the actual supply of the additional credit card numbers, this will not cause any difficulties to the credit card provider. For example, with a standard master credit

card number, there are up to fifteen or more digits, the first of which is used to identify the credit card provider, e.g., American Express®, VISA®, Mastercard®, etc. For major banks, three digits are used to identify the issuing bank. The last digit in a typical sixteen digit master credit card number is a checksum used to confirm that the number is a valid number. This leaves a total of up to 11 digits or more for the account identifying number and the expiration date. In some instances, the expiration date may not be sent back for clearance, while with certain credit card providers, additional credit card numbers or even additional information is required for clearance. For example, certain credit card providers print additional numbers on the card, which additional numbers are not embossed on the card and do not form part of the master credit card number. These additional printed and non-embossed credit card numbers can be used to identify that the person proffering the card for a non-card present transaction is actually in possession of the card when the order is made whether it be in writing or by phone. There are many devices, digits, pieces of information, etc. used by a credit card issuer or processor working for a credit card issuer to clear the credit card for the specific transaction. According to another embodiment, when issuing additional credit card numbers in accordance with the present invention, such additional credit card numbers could include a code which would identify that the person using the additional credit card number in a remote transaction is the one to whom the numbers were sent or, in the case of a disposable credit card, is the one to whom the disposable credit card was sent.

A preferred feature of these additional credit card numbers is that they be constrained to be in the correct format for a credit card number with a valid check sum, while at the same time be mathematically unrelated to each other or to the master credit card. In certain situations, for single use numbers, the expiration date is virtually irrelevant. Thus, using the month code of the expiration date with said eleven digits, there are 12×10^{11}, i.e., 1.2×10^{12}, i.e., 1,200 billion possible unique codes available for any given credit card provider. This would allow for 50 transactions a month for 10 years for 200 million account holders, before any codes would have to be recycled or a new header code introduced. When it is understood that there are then another 10^4 header numbers that a credit card provider can use, it will be appreciated that the structure

and arrangement of existing master credit card numbers is sufficient to operate this invention with the advantage that the existing infrastructure of dealing with credit card transactions can be used with minimum modification. All that is required for the credit card provider is to store the generated numbers against the master credit card number or other type of account number.

If, for example, the card is a VISA® card, there are approximately 21,000 issuing banks. The sixteen digit number has a "4" followed by a five digit code to identify the card issuer. The last number is a checksum to verify that it is a valid number. As a result, there are $21,000 \times 10^9 \times 12$ (252 trillion) unique numbers and associated expiry months. This number of codes is sufficient for 36,000 years of transaction processing at the current annual rate of approximately 7 billion transactions per year.

While existing credit card formats allow for a sufficiently large number of available card numbers, numbers will eventually need to be recycled for allocation. As the range of available numbers reduces in size over time, additional or recycled numbers should be added back into this range to ensure that the allocation process is performed from a range sufficiently large to maintain random allocation. The length of time prior to recycling depends on the total number of available unique card codes available to an issuer and the number of transactions that use limited use numbers. Such recycling can only occur after a number has been invalidated for further use and is no longer valid for refunds. Once recycled, automatic fraud detection mechanisms that would normally be activated on the attempted reuse of a previously inactivated card need to be altered by removing the recycled number from the list of previously issued limited use numbers.

The use triggered condition subsequent limitations placed on limited use card numbers, i.e., transaction value limitations, number of transactions limits, etc., are central to their additional flexibility and security compared to conventional credit/debit/charge cards. These limitations can be imposed and controlled in a variety of ways. For example, the limitations can be stored within a database held by the card issuer and used to check that the transaction falls within these limitations during the

authorization process.

Fig. 4 is a flow chart illustrating an exemplary process for limiting the use of a credit card number. A CPU can allocate a credit card number to a master credit card number (step 402), and allocate a condition to the credit card number. (Step 404). The CPU can then store the condition in a database of conditions. (Step 406). These limitations can be assigned by the issuer in a predetermined manner or can be imposed according to the requests of the card holder. These limitations can be encoded with the limited use numbers when the numbers are issued to a user so that the user can determine the limitations associated with a particular card. These limitations can be altered once a number is issued by updating the issuer database and the user maintained list of numbers. Communication between the user and card issuer to make these changes can be posted, conveyed verbally or electronically. (Step 408). When the card is used for a transaction (step 410), the transaction details are compared by the processing software with the limitations and the transaction is authorized only if the transaction falls within these limitations. (Step 412).

Alternatively, the limitations can be encoded within part of the number format that is transmitted during a transaction. The limitations would then be decoded from the transmitted transaction details by the card processor. This would offer the user more control, but would offer less security since knowledge of the encoding format could be used to fraudulently alter the limitations chosen by altering the appropriate portion of the limited use number format.

As Internet commerce develops, there will be an increased need for a wide range of financial transactions. The limitations placed on limited use card numbers can be used to implement a wide range of payment options. For example, a credit card number can be limited to a single transaction for a pre-arranged transaction limit. Or alternatively, a credit card number can be used, for example, to implement an installment plan where the credit card number is, for example, only valid for twelve payments for a pre-arranged transaction limit for twelve months to a single merchant. This plan provides security against fraud because it is locked to a single merchant,

and it is only good for one year. Or similarly, a credit card number can be used to implement a debit plan where the credit card number is limited to a specific merchant.

When the limited use number is limited to a specific merchant, the merchant can be prearranged by the user or can be determined by first use. In this situation a limited use card can be used to generate an account specific to a single merchant. For example, this can be used in situations on the Internet where a web merchant will retain a credit card number for later purchases. By being limited to a single merchant, theft of the number from the merchant's computer systems will not allow the card to be used elsewhere. Also, any such use will immediately identify a specific merchant as having suffered a security breach. Determination-by-first use could involve linking the merchant name or credit card system identification number at the time of making the purchase, during the authorization process or during the settlement process.

Or finally, a credit card number can be used as a gift voucher where the credit card number is limited to a specific transaction value or limit, but it can be used for any merchant. A gift voucher limited use card could also have a pre-determined limitation to a specific merchant or a type of merchants or to a group of merchants such as within an "online shopping mall".

The next matter that is considered is how these additional credit card numbers and/or additional credit cards are distributed to a credit card holder. One way of providing such additional credit card numbers and/or additional credit cards is to in some way provide them physically to the master credit card holder, whether it be by collection, delivery by courier, post or some other way which can generally be covered under the heading of provision by post. Obviously, the financial institutions wish to provide the additional credit card numbers or the additional credit cards to the user as efficiently as possible with the minimum risk of the additional credit card numbers and/or cards falling into a third party's hand. While one can never prevent theft, for example, of a credit card from a user, what is important is to ensure that these disposable credit cards and/or credit card numbers are delivered to the user with the least possibility of a third party obtaining either the numbers or the disposable credit cards from the time

they are generated until the time they are physically received by the user.

It is envisaged that there are various methods by which a credit card provider could issue the additional credit card numbers and/or credit cards to the user. One of the simplest ways would be to post them on request. Another way would be for the credit card provider, after receiving a payment of an account or with a statement of an account, to provide a sufficient number of additional credit card numbers and/or additional credit cards to replace the ones used since the previous statement. Particularly, if such statements do not quote the master credit card number or some code number, it would be possible to put in additional checks on the activation of the additional credit card numbers or credit cards. Some form of receipt system could be used. In this way effective theft would be reduced.

Fig. 5 is a flowchart illustrating an exemplary process for distributing credit card numbers. A credit card issuer allocates a master credit card number or more generically a type of master account number to a master credit card or account owner. (Step 502). The credit card issuer then allocates limited use numbers to the master account number. (Step 504). For pre-prepared cards, the card issuer can decide whether to print (or incorporate by some other means such as embossing) one number per card or multiple numbers per card. (Step 506). The card issuer can distribute multiple numbers using a single card (step 508) or distribute multiple numbers using multiple cards. (Step 512).

In either case, it is important that the user can keep track of which numbers have been used. If the card has only one number, an opaque removable cover can be used to cover one or more portions of the card. (Step 510). For example, the opaque removable cover can cover the number portion of the card, so that the cover has to be removed before the card can be used. The act of removing the cover indicates that the card number has been accessed or used.

Or alternatively, an opaque removable cover can conceal a message such as "used." The opaque removable cover can be a scratch off layer that is scratched off before or

after the card is used. The scratch off layer can resemble the layer that is often used to cover lottery numbers or the like. Or alternatively, the single use cards can be placed in a self-contained container that resembles a razor blade dispenser. (Step 516). The owner can remove a single use card from a first compartment and then place the used card into a second compartment.

If the card has multiple numbers, the owner can keep track of the numbers by using a device that covers one or more portions of the card. (Step 510). The device can cover the numbers until they are used. As described above, the device can comprise multiple opaque layers that must be removed prior to the use of each number. Or alternatively, each number could be visible when the card is issued and each number is associated with a panel in which an opaque covering conceals a message that indicates that the number has been used. After each use, the corresponding covering is removed or scratched off to indicate that the number has been used.

In both above cases the solutions incorporated on the cards act to remind the user which numbers have been used. The critical check on the validity of the number is performed by the processing software responsible for authorizing card transactions.

The additional credit card numbers and/or cards can be sent with a statement. (Step 518). The additional credit card numbers are not activated until the statement is paid. (Step 520). The card issuer could also require that the payment be accompanied by the master credit card number or another identifier. Or, for example, an additional security step involving either direct contact with the issuing credit card company or an independently issued password to allow activation of an electronic device could be used.

A further way in which the additional credit card numbers and/or additional credit cards could be distributed to the user is by way of an ATM machine. (Step 522). The ATM machine with very little modification could provide the additional credit card numbers. Similarly, with relatively little modification, an ATM machine could provide additional credit cards.

Cards/single use numbers can be issued directly into an electronic device that is capable of storing such numbers. This applies to mobile phones and pager devices to which information can be transmitted using existing systems and computers connected either directly or via a telecommunications system to the Internet or a specific host computer system. In such a situation a mechanism is required to protect these numbers in transit to prevent unauthorized access. For global applications, this mechanism must not be subject to export restrictions. In addition, this protection should not be susceptible to "brute force" decryption techniques. Such a system is described below in relation to the storage of single use cards.

An alternative method to provide additional credit card numbers could be by way of a computer programs. Obviously it would be necessary for the credit card provider to have sufficient security that when the computer program was dispatched, either through the telecommunications network or through the post, that unauthorized access could not be obtained.

In the situation where the user stores and accesses limited use numbers via an electronic device such a computer of any form (desktop, television or cable linked Internet access device, laptop, palmtop, personal organizer, etc), any device that can deliver the same functions as a computer or dedicated Internet access device, a dedicated microprocessor device with key pad and screen or any form of telephone with associated microprocessor controlled electronics, the associated software can perform some or all of the following functions:

1) Password controlled access to software or other security activation system that can verify that the user has a valid right of access.
2) Secure storage of issued limited use credit/debit/charge card numbers until required by the user. These numbers can be stored in a variety of encrypted forms. An additional security step is to encrypt the number in the form a valid credit card number as previously described.
3) Secure storage of transaction details and date of use for reconciliation with

— records held by the credit/debit/charge card company in case of disagreement. This may include digitally signing each transaction record.

4) Facility for user to review past usage of limited use card numbers and transactions.

5) Notification to user of available number of limited use cards.

6) Initiate automated request from software to card issuing organization or agreed agent for further cards to be issued by previously agreed route if requested by user or if the number of available limited use cards is less than a pre-arranged limit.

7) Secure communication between software package and card issuing organization or agreed agent for downloading additional limited use numbers. This secure communication can exploit any available form of encryption suitable for this purpose.

8) Secure communication between card issuing organization or agreed agent and the software package for the transmission of information regarding credit card transactions, account balances and other information as requested by the user or card issuer. This secure communication can exploit any available form of encryption suitable for this purpose.

9) Automated or manual means for transfer of credit card information to the merchant. The software can integrate with Internet software in the situation where it is run on a device linked to the Internet or similar electronic network and allow automatic transmission of transaction details if the merchant software so allows. To ensure compatibility with any form of merchant software the user also has the option of dragging and dropping a limited use number displayed by the software onto the appropriate part of a web page, or manually entering the number. In the case a device intended for use over the telephone, the number can either be spoken by the user or appropriate tones can be generated to automatically transmit the number to the merchant.

10) Use of digital signature verification to verify both parties of a credit card transaction (i.e. merchant and cardholder).

11) Use of digital signature verification to verify both parties of a communication involving the transmission of financial information or additional limited use card

— numbers (i.e. card issuer and cardholder).

12) Use of stored lists of limited use numbers held by user and card issuer as dynamic passwords to verify both parties (user and card issuer) of a communication involving transmission of financial information or additional limited card numbers.

For "card not present" transactions, it is proposed that the customer uses an electronic device to store issued single use numbers. This may represent a range of devices from a mobile telephone, pager, dedicated single use storage device or a software package that can run on range of platforms such as a conventional desktop computer, television based Internet access device (e.g., WebTV) or a portable computing device.

The software that is used within these devices for storing and accessing these numbers will have specific features that are common to all platforms/devices.

For security reasons, access to the software will be password protected or protected by another security system that allows identification of the user (e.g., magnetic stripe card reader, chip card reader, electronic token generator, fingerprint recognition system or the like). Multiple passwords may be employed to provide limited access to certain individuals, for example limiting access for a family member to single use numbers with specific pre-allocated limits on application or maximum transaction value.

The single use numbers are preferably stored in a secure form involving one or more encryption systems. It is proposed that a dual system will be employed using a standard protocol (e.g., DES or RSA encryption) and a specific system designed for credit cards as described below.

"Brute force" decryption involves using multiple fast computers and specific algorithms to test large numbers of possible encryption "keys." Success can be determined by seeing whether the result appears in the expected format, for example as

comprehensible English text in the case of an encrypted document. If the encrypted version is in an identical format to the unencrypted version (though with different information) then brute force decryption cannot succeed. This is not a computationally viable option for text but it is possible for credit cards.

The approach is to break down each component of a credit card number and encrypt these with a private password so as to maintain the numerical composition of each component. The end result should be securely encrypted but should not represent another existing credit card account. This can be achieved by constraining the encryption system to convert the credit card header sequence used to identify the issuing bank (usually 4-6 digits) into a currently unused sequence. Since this information will be constant for all cards from the same issuer, this information should be randomized (rather than encrypted) to prevent recognition of a valid decryption solution. Once the rest of the number is decrypted by the program, the appropriate header sequence can be added. The remaining digits excluding the checksum (the last digit) are then encrypted using any private key encryption system that will maintain the same number of digits and produce a result that represents the numerals 0 to 9. The expiration date and any other identifying digits are also encrypted in such a manner as to respect their existing structure, i.e., the month is encrypted between 1 and 12 and the year is encrypted so as to represent a number within the next three years that ensures that the expiration date is valid. Following these steps, the digits used to calculate the checksum in a normal card number are processed to calculate a valid checksum for the encrypted card. The result is a valid appearing credit card number that has a valid checksum and which can be guaranteed not to belong to any existing credit/debit card account holder.

For example, for a card with a 6 digit header and valid checksum, e.g., "1234 5678 9012 3452 expiration date of 12/99," 123456 is randomly assigned to a currently unused header sequence, e.g., 090234 (this is an example and does not necessarily represent an unused header sequence). 789012345 is encrypted into another 9 digit number, e.g., 209476391. 12/99 is encrypted to a valid date format that ensures the card is not expired, e.g., 3/00. The checksum is recalculated to

produce a valid appearing credit card number, for this example the checksum is 4, i.e., 0902 3420 9476 3914 expiry 3/00.

To decrypt this number for use or after transmission from the bank, the appropriate header sequence for the issuer is exchanged for the digits in the encrypted number. The other digits are decrypted using the private password and the check-sum is recalculated.

Provided that the header number is unused and the private password remains private, then this number is encrypted in such a way that brute force encryption cannot be used to determine the original number, since it will not be possible to determine when the correct solution has been reached. In combination with standard encryption systems, this allows a means to securely store credit cards and transmit them over insecure systems with confidence.

Once the appropriate password is entered into the software, the next available single use number is decrypted and either displayed, allowing the customer to use it in any form of trade that can achieved by quoting credit card information, or directly transmitted via the software to the merchant. Once used, the single use number is removed from the stored list. The date of access, the number accessed and any additional available transaction details are then stored in a secure fashion and digitally signed to allow for verification in the case of a disputed transaction. Each access to a single use number requires the entry of a password to prevent unauthorized access if the customer leaves his software/computer device unattended and active.

Other types of encryption may also be used, for example, which require the use of a mask and/or private key. For example, as described above, this approach also breaks down and encrypts each component of a credit card number so as to maintain the numerical composition of each component. Similar to that described above, the bank identifying header sequence, e.g., in the case of VISA ® cards, the initial digit "4" followed by the 5 digit BIN number, is replaced with an equal number of random digits taken from the range of unused headers. This ensures that the resulting number does

not represent some other valid existing credit card number. These replacement header sequence digits can be fixed for a given card issuer and can be reconstructed after decryption.

The final checksum digit can be handled in one of several ways. For example, the checksum digit can be recalculated based on the encrypted remaining digits as described above. Alternatively, the final checksum digit can be omitted from the encryption process and recalculated after decryption.

The remaining digits can be reformatted into another number with the same number of digits by any reversible encryption process. The same process may also be applied to all other numerical information transmitted that may be issued during a transaction, e.g., the expiry date and other codes. One process for randomizing these remaining digits is described above. Another process to encode the remaining digits is to perform a digit by digit mathematical operation in combination with a mask containing the same number of digits as the remaining digits to be encoded.

For example, assume the original remaining digits are 878918982 and the random mask digits, containing the same number of digits as the remaining digits to be encoded, are 143337658. A modulo 10 arithmetic function is then performed using the original remaining digits and the random mask digits as follows to achieve the encrypted result.

Original remaining digits	8	7	8	9	1	8	9	8	2
Random mask digits	1	4	3	3	3	7	6	5	8
Encrypted remaining digits	9	1	1	2	4	5	5	3	0

After transmission of the encrypted card number, including the replacement header sequence digits, the encrypted remaining digits and the checksum digit, if appropriate, the encrypted card number is separated out into its components. The encrypted remaining digits are decrypted in the opposite manner in which they were encrypted.

Specifically, knowing the random mask digits and the encrypted remaining digits, a modulo 10 subtraction is performed to reconstruct the original remaining digits as follows.

Encrypted remaining digits	9	1	1	2	4	5	5	3	0
Random mask digits	1	4	3	3	3	7	6	5	8
Original remaining digits	8	7	8	9	1	8	9	8	2

Even with this simple encryption technique, the decryption solution requires access to the private key because the solution cannot be identified in isolation. In addition, this process enables the reconstruction of one of the sequences, i.e., the original remaining digits, the random mask digits or the encrypted remaining digits, knowing the two other sequences.

Fig. 6 is a flow chart illustrating an exemplary process for electronically using credit card numbers. The software can be launched either on its own or activated by an icon integrated into an Internet browser. (Step 602). The software can provide a simple interface with a graphical appearance that exploits familiar images of credit cards and/or ATM's. The software can be programmed using Java code or a Java core embedded in a c/c^{++} application or equivalent programming language.

Once launched the user puts in one password to gain access to the main screen which contains a key pad to allow a PIN to be inputted either by keyboard or by mouse clicks. (Step 604). The latter protects against any covert attempts to record passwords by trapping key strokes. A consecutive number of errors in inputting the password will permanently disable the program and overwrite remaining encrypted numbers. After the correct PIN is entered, the user can select a new limited use number with or without additional constraints (e.g. maximal transaction value). (Step

606). A new limited use number is then displayed on the graphical interface. The software can provide secure access to encrypted credit card numbers that are stored on a computer's hard disk. (Step 608). These numbers can be accessed for use on the Internet or for use over the phone/mail order. (Step 610). The numbers must therefore be able to be inserted directly into a web page (step 612), or printed out/copied from screen for use in other ways. (Step 614). The limited use number can be copied, printed, pasted via the clipboard (or equivalent) or dragged-and -dropped onto a web page. The length of time a number is displayed and how the program terminates are user configurable. The user can also record a comment to provide further information about how a number was to be applied. For automated transactions, the software should ideally be able to intercept and respond to merchant server initiated signals activating integrated functions within the browser.

Once a number has been accessed, it can be deleted from the encrypted lists. (Step 616). The date, number, current URL in the case of Web use and any user comments are then stored by a separate form of encryption to facilitate audit/review. (Step 618). The user can review, but not edit this information

There should be a facility for downloading additional numbers either from additional floppies or via the Internet using high security protocols. (Step 620). The latter function can be performed by a separate program.

The program should include a maximal degree of transparent security features, i.e., features that do not affect a normal user, but that protect against the program being reinstalled or copied onto a second machine. This means that the encrypted limited use numbers should either be stored within the executable file or stored in a file that also stores encrypted copies of the machine specific information. (Step 622). This is required to ensure that the numbers can only be accessed on the machine on which the software was first installed. The data files should also be stored as hidden system files.

Some users may wish to have the equivalent of an electronic wallet that can be de-installed from one computer and reinserted on another, for example, when transferring a "wallet" from an office to a home machine. This transfer process ensures that only one version of the program is running at any one time and that no problems arise in terms of reconciling lists of used numbers. Appropriate security mechanisms can be implemented to identify the valid user.

Appropriate security measures include encryption. Encryption of limited use numbers should involve two levels as exemplified above. At the first level, the card numbers are encrypted using an algorithm that acts only to alter the free digits within the credit card. The header sequence (i.e., BIN number) is left unaltered or converted into an unused BIN number and the checksum recalculated. This prevents any form of brute decryption because there will be no way of telling when the correct algorithm has been selected since each number starts and ends up as a valid looking credit card number. Following this step each number is encrypted with industry standard encryption methods (e.g. RSA or DES). Following decryption within the program the checksum is recalculated for the final number and the appropriate bin number reinserted.

The software can be shipped on a single 1.4 Mb Floppy (or any other computer readable or usable medium) in an encrypted form or downloaded from a website. Limited use numbers can be issued either with the program or independently. An independently shipped password can be required for installation. The installation process will allow the program to be installed a restricted number of times after which critical data is overwritten. The precise number of allowable installations will be easily alterable within the software design. Once installed on the host computer, the program encrypts internal information regarding the machine's configuration to protect against copying of the program onto other machines. At first installation the user can select his own passwords. These will be used to control both access to the programs and to influence the pattern of one level of encryption that is applied to limited use numbers.

As numbers are accessed, a graphical indicator of the remaining amount of limited use numbers provides early warning if additional numbers are required. The software can also provide a log of previously accessed numbers, the date, associated URL if activated from within a browser and comment; a summary of account expenditure; assistance with adding additional numbers from disk or via Internet; the ability to configure additional passwords/users for shared cards; and/or hot link Internet access to the card number issuer's web site.

It is envisioned that additional credit card numbers and/or additional credit cards would be processed by merchants in the same manner as existing credit card numbers and/or credit cards with the merchant obtaining validation of the credit card number from the credit card company or authorized third party. In much the same way as at present, the additional credit card number would be matched to the customer account and the account would be debited accordingly. The merchant reimbursement following verification of an additional credit card transaction would be performed in the normal manner. A particular advantage for the merchant is that since they are never in possession of the master credit card number or indeed, in many instances, of the master credit card, they have no responsibility for security to the master credit card holder. It is envisaged that where there are additional credit cards used, it may not be preferable to take an imprint of the credit card manually, as the imprint can be taken electronically. Similarly, those processing the credit cards will process them in the same manner described heretofore.

Processing systems for handling limited use cards perform a number of functions including some or all of the following:

1) Verify that the limited use number is valid.

2) Verify that the transaction falls within limitations placed on the specific number.

3) In the case of a limited use number associated with another account, verify that transaction falls within limits acceptable for the associated account.

4) Provide authorization to the merchant if valid and within the limitations for specified number and associated account.

5) Permit later transactions to be charged to a limited use number that has been invalidated for further authorizations only if the transaction is generated by the same merchant that obtained pre-authorization for the same transaction.

6) Deny authorization if invalid or exceeding limitations on number or associated account.

7) Activate fraud detection mechanisms if invalid number or on attempt to reuse an invalidated limited use number.

8) Invalidate limited use number for further authorizations/payments if limitations on use are met or exceeded by a specific transaction.

9) Maintain list of invalidated numbers for reimbursement in the case of returned or faulty goods for a defined period.

10) Limited use numbers and transaction details logged and linked to associated account.

11) Transmit records of limited use and other card transactions to the user by post or e-mail.

12) Instigate payment to merchant for approved transactions.

13) Instigate reimbursement to account holder in case of a refund.

14) Invoice account holder for payment for charges incurred or arrange settlement via another account.